

DOMAIN NAME SYSTEM

After reading this chapter and completing the exercises, you will be able to:

- ◆ Provide an overview of the Domain Name System (DNS)
- ◆ Describe the features of DNS in Windows 2000
- ◆ Install the DNS service
- ◆ Configure a DNS server
- ◆ Create resource records manually
- ◆ Configure a client to use DNS
- ◆ Manage, monitor, and troubleshoot DNS

In order to communicate on TCP/IP networks, clients must resolve host names to IP addresses. On very small networks, static hosts files may be used to map the host name to an IP address. Most networks, however, need Active Directory installed, which must use DNS servers to handle host name to IP address resolution. This chapter introduces you to the DNS service as a prelude to actually installing and configuring a DNS server on a Windows 2000 network. In this chapter, you also learn to manage, monitor, and troubleshoot the DNS service.

DOMAIN NAME SYSTEM OVERVIEW

Host names are simple names used as aliases for IP addresses. Early in the development of TCP/IP, researchers realized that humans are much more adept at remembering names than numbers.

As a result, the TCP/IP protocol stack developed with the idea that computers on a network would have host names that could be used to access resources such as files and printers. Unfortunately, computers are much better at numbers than names. Host files and DNS perform the task of translating from names (host names) to IP addresses.



The **hostname** command entered after the command prompt returns the currently configured host name on the computer.

Hosts Files

The ability to perform host name to IP address resolution is an extremely important task on a TCP/IP network. Without host name resolution, users cannot access Internet or intranet resources via Fully Qualified Domain Names (FQDN). For example, *www.course.com* is the Fully Qualified Domain Name for the Web server for Course Technology: *www* represents the host name, while *course.com* is the domain name. FQDN makes Internet resources accessible with easy-to-remember names used instead of IP addresses.

Windows 2000 provides a variety of methods to perform host name to IP resolution, but, in the end, the **Domain Name System (DNS)** is the resolution method of choice on all Windows 2000 networks.

Originally on TCP/IP networks, hosts used a text file called a **host file** to perform host name to IP address resolution. When the Internet consisted of 30 or 40 computers, manually editing the host file was not a labor-intensive task. Host files have a specific format. The following example is the host file available in Windows 2000 in the systemroot\system32\drivers\etc folder.

```
# Copyright (c) 1993-1999 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for
#Windows.
#
# This file contains the mappings of IP addresses to host
#names. Each entry should be kept on an individual line. The
#IP address should be placed in the first column followed by the
#corresponding host name.
# The IP address and the host name should be separated by at
#least one space.
#
```

```
# Additionally, comments (such as these) may be inserted on
# individual lines or following the machine name denoted by a
# '#' symbol.
#
# For example:
#
#       102.54.94.97      rhino.acme.com      # source server
#       38.25.63.10     x.acme.com         # x client host

127.0.0.1 localhost
```

In the sample host file, the # symbol is used to mark and allow for comment lines within the host file. To add an entry to the host file, you must type the IP address of the host and then the host name or Fully Qualified Domain Name of the host. For example, to add and to comment on an entry for the host 192.168.1.21, you place the following in the host file:

```
192.168.1.21 example.win2kbook.org #sample entry for a host
```

Host files in Windows 2000 must be stored in the %systemroot%\system32\drivers\etc directory. (winnt is the default path for the systemroot directory.) Because entries need to be added manually to the host file, it is not a practical method for host name resolution on anything but the smallest of networks. However, if your network is very small and you do not want to spend the money or take the trouble to install and configure DNS, a host file is a viable alternative for host name to IP address resolution.

Windows 2000 provides six different ways to perform host name to IP address resolution. Figure 4-1 displays the six support methods for host name resolution in Windows 2000.

The local host name is the first item a Windows 2000 machine checks when trying to resolve an IP address to a host name. If the local host name is the same as the host name being resolved, resolution occurs very quickly and efficiently. If, however, the local host name and the host name to be resolved are not the same, the Windows 2000 machine attempts to locate a host name to IP address mapping in the locally defined host file. If no resolution occurs using the host file, the Windows 2000 machine contacts the DNS server specified in its static IP address settings or in the DNS entry it receives from a DHCP server. If no resolution occurs via contacting the DNS server, the Windows 2000 machine tries a fourth method: it falls back on NetBIOS naming resolution methods by contacting a **Windows Internet Name Service (WINS)** server to attempt to find a mapping between the host name and an IP address. Using the final two methods, the client attempts to resolve the host name via either a broadcast or the **LMHOSTS** file, a text file that maps NetBIOS names to IP addresses. (Chapter 5 discusses NetBIOS names and name resolution.)

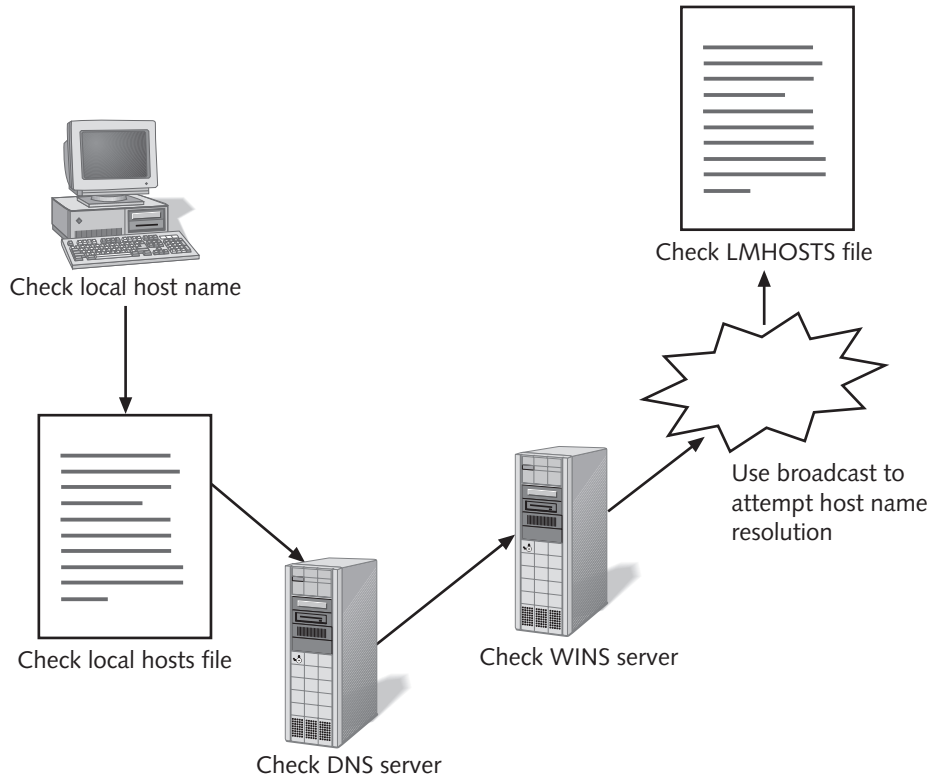


Figure 4-1 Six methods for host name resolution in Windows 2000

DNS Structure

In most host name resolutions on Windows 2000 networks, the client resolves host name to IP address mapping by using a local host name lookup, the local host file, or more than likely, a DNS server. The Domain Name System that supports the operation of all DNS servers is a hierarchical naming system. The DNS hierarchy consists of the root-level domain, top-level domains, second-level domains, subdomains within the second-level domains, and resource records such as host names. Figure 4-2 displays the DNS naming hierarchical structure.

The root-level domain is the highest level in the DNS hierarchy. It is represented by a period, which is usually not shown on Fully Qualified Domain Names.

Top-level Domains

Top-level domains are the organizational domains created by the designers of the Internet to simplify the naming and logical structure of the DNS namespace. Figure 4-2 shows the .gov, .com, and .org top-level domains. Table 4-1 shows several of the top-level domains and the areas they represent.

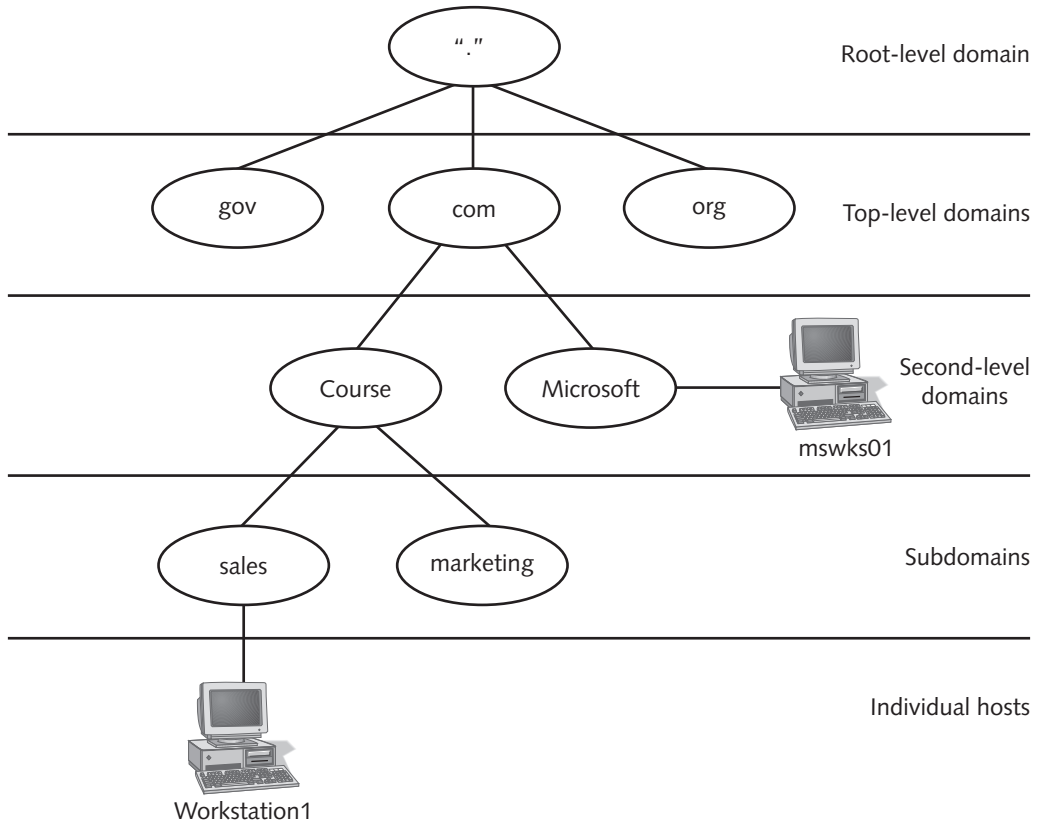


Figure 4-2 DNS hierarchical structure

Table 4-1 Top-level domains

Top-level Domain	Areas Represented
gov	U.S. government agencies (does not include most military services)
com	Commercial organizations
mil	U.S. military services
edu	Educational institutions
net	Internet Service Providers (ISPs)
org	Nonprofit organizations

The list in Table 4-1 is not complete. Top-level domains also exist for most countries, and new top-level domains will be introduced in the very near future.

Second-level Domains and Subdomains

Second-level domains are found beneath the top-level domains. It is at the second-level domains that most companies register their names with a **name registration company**, a

company with the ability or authority to add second-level domains. In DNS, any company with **authority** over a particular portion of the DNS namespace can add domains to that space. Since name registration companies can add second-level domains, you must contact them to register a particular second-level domain name. For instance, Course Technology had to contact a name registration company to obtain the second-level domain name `course.com`. Once Course Technology registered and created `course.com`, it was said to have authority over that domain. Having authority allows Course Technology to create subdomains to divide the domain namespace further. DNS servers located within the Course Technology company have the `course.com` domain as their **zone of authority**, the portion of the DNS namespace for which a name server is responsible. The ability to be authoritative for the `course.com` domain allows the creation of subdomains such as `sales.course.com` and `marketing.course.com`.

Subdomains such as `sales` and `marketing` found in Figure 4-2 further divide second-level domains. Most companies use subdomains to create smaller administrative units in the DNS namespace.

On the lowest level of the DNS namespace are the actual resource records such as host names. In Figure 4-2, you can see that hosts (and therefore host names) reside at either the second-level domain or within subdomains. The host `mswks01` in the Microsoft second-level domain is a computer in the `microsoft.com` domain. The host `Workstation1` is a computer in the `sales` subdomain of the `course.com` second-level domain.

DNS Zones

Within DNS are the levels of domains depicted in Figure 4-2, along with a concept known as **DNS zones**. DNS zones are portions of the DNS namespace that can be administered as single units. Each zone has a **primary name server** that holds the **DNS zone file**. For each zone in which a primary DNS server holds the main DNS zone file, that server is considered authoritative for that portion of the namespace. Figure 4-3 shows the `course.com` domain and the authoritative server for each portion of the namespace.

In Figure 4-3, each server in the domain or subdomain is considered the primary name server for that portion of the DNS namespace. In each case, the DNS servers as primary name servers hold the read/write master copy of the DNS zone file for that domain or subdomain. **Primary name servers** hold a read/write copy of the zone file. In other words, changes to the DNS zone file only occur on primary name servers. **Secondary name servers** are DNS servers configured to hold a read-only copy of the primary name server's DNS zone file. Windows 2000 DNS primary servers replicate and send the information in the file to the secondary name servers at predefined intervals. Windows 2000 DNS also supports incremental zone transfers. When changes occur in the DNS database, Windows 2000 DNS primary servers send only the updates to configured secondary servers. Updates on Windows 2000 DNS servers are faster, thus reducing network traffic and consolidating network bandwidth. Previous versions of Windows DNS servers sent the entire DNS file when changes occurred.

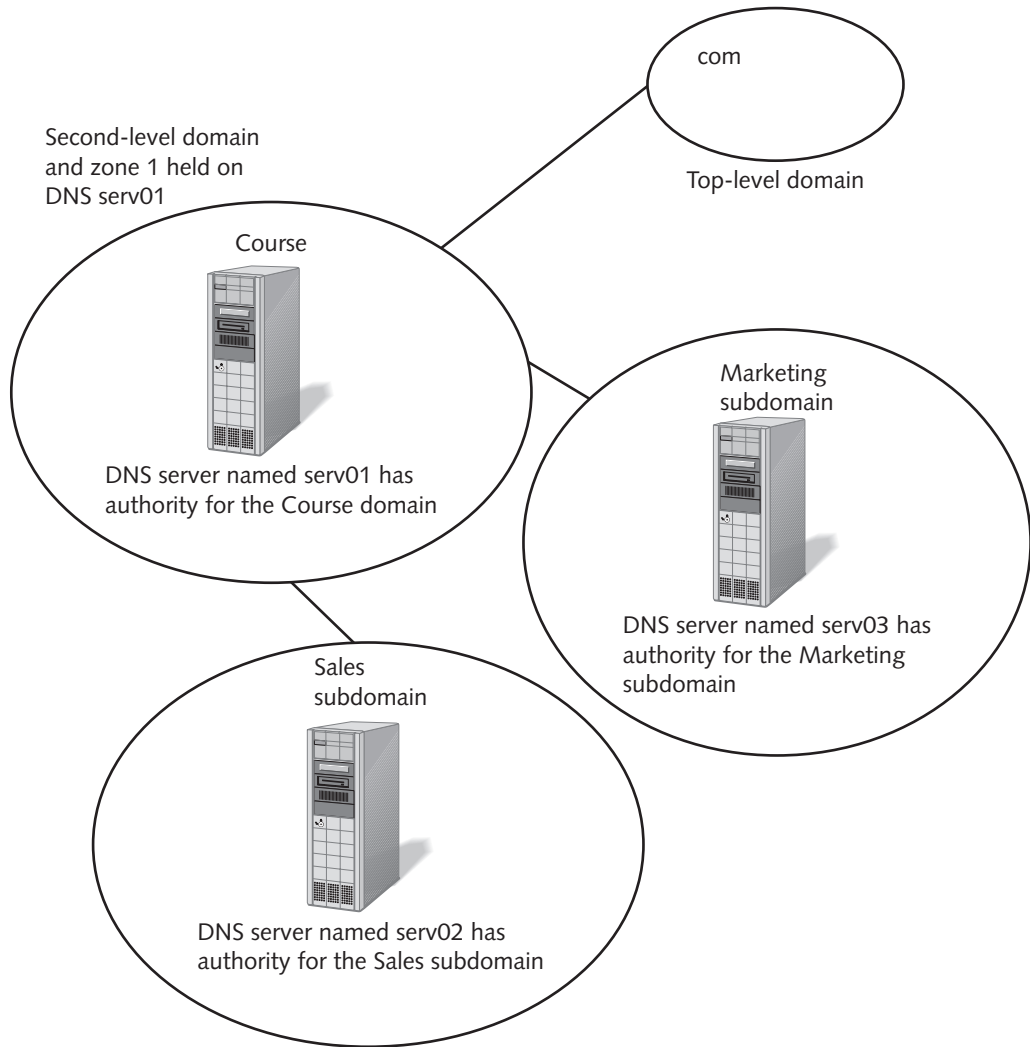


Figure 4-3 Zones of authority

All networks should minimally have a primary and a secondary DNS name server, or two DNS servers configured to use **Active Directory integrated zones**, which have DNS information stored and replicated using Active Directory. In addition, DNS servers can also be configured as caching-only servers. **Caching-only servers** hold no primary or secondary zone file for any particular portion of the DNS namespace. Instead, they build a cache of information from DNS resolutions they obtain from other primary or secondary name servers. Caching-only servers are good for areas that do not need a full secondary server or that do not have enough bandwidth to support **zones transfers**. Caching-only servers are ideal for remote offices connected to the central office via slow-speed WAN links such as ISDN.

DNS servers hold two types of DNS zones: forward lookup zones and reverse lookup zones. **Forward lookup zones** contain host name to IP address mappings. In other words, when a client has the host name of a destination computer and needs the IP address to complete communication, it receives that information from forward lookup zones. **Reverse lookup zones** contain IP address to host name mappings. A client that has the IP address of the destination computer and needs the host name uses reverse lookup zones to find an IP address to host name mapping. Reverse lookup zones are used many times to verify that an IP address is from a certain area or country. Using the IP address and a configured reverse lookup zone, DNS clients can determine in which DNS domain a computer resides.

To understand the DNS resolution process, you must first understand the two roles available to computers in the DNS system. In DNS, computers can be DNS servers that answer client requests or DNS resolvers, clients that initiate requests. Three types of requests or queries exist: recursive, iterative, and inverse. A DNS client sends a **recursive query** to a DNS server, which must directly answer the query. In a recursive query, the DNS server must respond with the best answer that its zone files currently have. To search higher up into the DNS namespace, DNS servers can use iterative queries. **Iterative queries** allow DNS servers to learn DNS information from other DNS servers. DNS servers use iterative queries to search for and find the DNS server with authority over the portion of the DNS namespace within which the requested host resides. This authoritative server responds to the iterative query with the host name to IP address mapping or a referral to another name server in the DNS domain that has authority. **Inverse queries**, the third type of query, find a host name from a known IP address. In other words, the client knows the IP address, but it needs to find the host name. Inverse queries use the reverse lookup zones, also known as **in-addr.arpa**.

Resource Records

Within the actual zone files, resource records are used to point to particular resources such as hosts, mail exchangers, and name servers. Table 4-2 lists many of the most common resource types. Later in this chapter you will learn how to create individual resource records.

Table 4-2 Common resource records

Resource Record	Use
SOA	All DNS zones begin with a Start of Authority (SOA) record that displays informational items such as the name of the authoritative server for that zone, the Time to Live (TTL) for zone records, and the e-mail address of the person responsible for the zone.
A	Provides host name to IP address mapping
NS	Name server (NS) record specifies the names of servers authoritative for a domain.
CNAME	Canonical Name (CNAME) allows an alias to be given to a machine that already has an A record entry. Canonical names allow machines to use common names such as <i>www.course.com</i> instead of <i>win2kweb.course.com</i> .

Table 4-2 Common resource records (continued)

Resource Record	Use
MX	Mail exchanger (MX) record specifies the mail servers considered authoritative for a particular domain.
SRV	Service (SRV) record is new to the Windows 2000 DNS service. Domain controllers add an SRV record to the DNS database automatically so clients can locate the domain controllers for services such as long on, resource permissions, and other network services. You can also add other service records to point to services running on particular servers.
PTR	Pointer (PTR) records are the IP address to host name mappings used to perform reverse lookups.

Windows 2000 DNS

The DNS server service that ships with Windows 2000 fully supports all parts of DNS mentioned in the overview section of this chapter. It also supports new features such as incremental zone transfers and dynamic DNS.

Unlike Windows NT DNS servers, Windows 2000 servers acting as primary DNS servers do not send the entire zone file to a secondary server. Windows 2000 sends just the changes in the DNS database. Sending only the changes instead of the entire database conserves network bandwidth.

The Windows 2000 DNS server also supports dynamic DNS as defined in RFC 2136. Dynamic DNS allows clients to register DNS information automatically with a DNS server. The implementation of DNS in Windows 2000 also supports dynamic registration of clients that do not support DDNS through the use of a service such as the Windows 2000 DHCP service.



The section, “DNS Client Configuration,” later in this chapter presents the proper steps to configure a Windows 2000 client to register DNS information dynamically. You will also learn the dynamic registration process provided by the Windows 2000 DHCP service for non-DDNS Clients.

INSTALLING DNS SERVICE

Installing the DNS service requires that you configure certain items on the server before loading the service.

First, the server must have a static IP address, subnet mask, and default gateway (if your network has multiple networks or subnets). Microsoft also recommends that you set the domain name suffix on the server before installing the DNS service. This allows the service to create correct initial resource records when you install it. (For example, for the publishing.course.com domain, the suffix is course.com. Figure 4-4 displays the correct dialog box for configuring the DNS suffix. You access this dialog box via the Advanced TCP/IP Settings dialog box on the DNS tab.

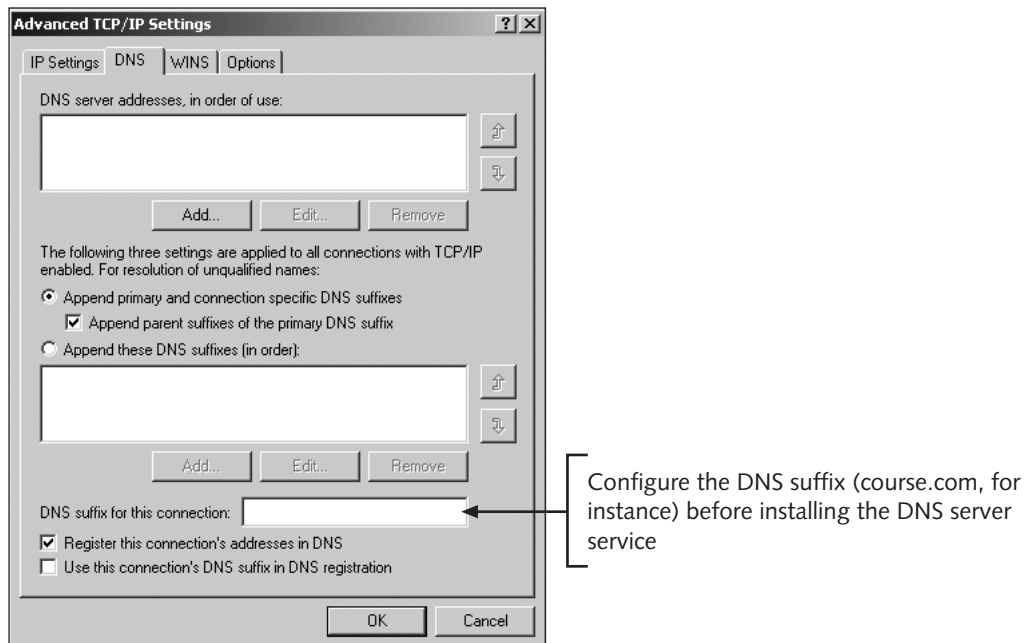


Figure 4-4 Domain name configuration

Once you meet these prerequisites, install the DNS server service with Optional Networking Components, accessible via the Advanced menu in Network and Dial-up Connections. Figure 4-5 shows the Windows Optional Networking Components Wizard dialog box.

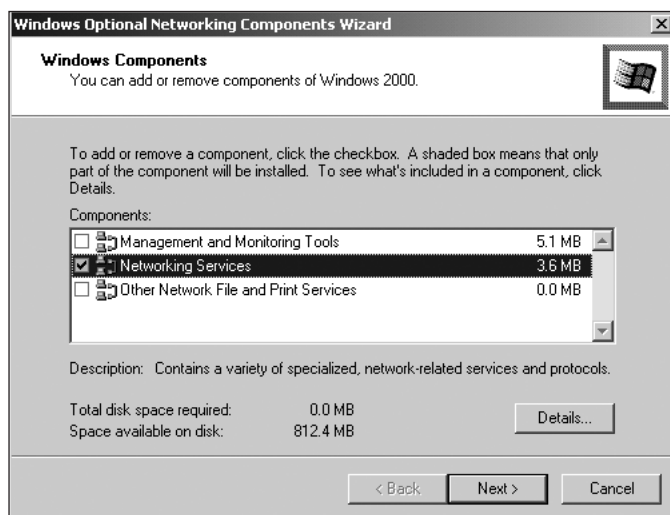


Figure 4-5 Windows Optional Networking Components Wizard

To install the DNS service, you must double-click Networking Services in the Windows Optional Networking Components Wizard and select the DNS service. Once you completely install the service, the DNS management console is added to the Administrative Tools folder under Start, Programs, Administrative Tools. Figure 4-6 shows the DNS management console.

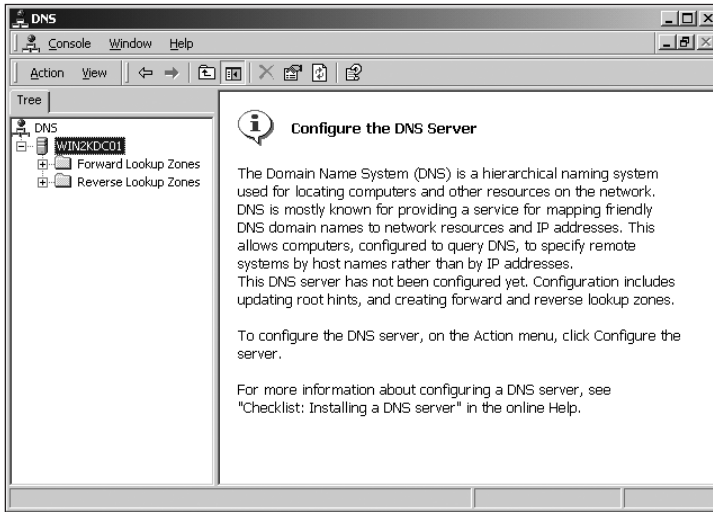


Figure 4-6 DNS management console

At this point you are ready to configure the DNS server service to act as a primary or secondary name server. If Active Directory is installed on your network, you have the option to create Active Directory integrated zones.



Another method of installing DNS is to install Active Directory first. If the DNS service is not installed, and you install Active Directory via the *dcpromo* command, you are prompted to install the DNS service or to configure it manually. Using the Active Directory install to configure DNS configures the DNS server with an Active Directory zone for use with AD.

CONFIGURING THE DNS SERVER SERVICE

Installing the DNS service may be easy, but configuration can become a very complicated task. In this section, you learn how to configure a root name server, primary zones, secondary zones, and caching-only servers. You also learn how to configure delegation for use with a subdomain. Finally, you learn how to configure the Windows 2000 DNS service to allow dynamic updates.

Configuring a Root Name Server

On networks not connected to the Internet or networks that cannot access the Internet's **root name servers** due to a firewall or proxy server, configuring a root name server for internal use may be necessary. If your DNS servers cannot connect to the DNS root servers, you must configure a root server on your machine for name resolution to occur correctly. Otherwise, your DNS servers may have trouble performing normal name resolutions.

To configure the root name server, open the DNS management console, right-click Forward Lookup Zones, and select New Zone. Figure 4-7 shows this process.

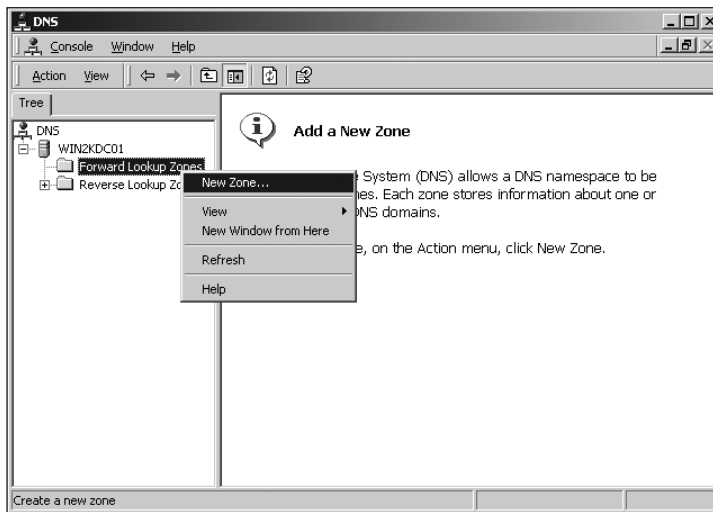


Figure 4-7 Configuring a new zone

The New Zone Wizard then starts and prompts you for a type of zone. Although you have options to create an Active Directory integrated zone (if AD is installed), primary zone, or secondary zone, you must choose a primary zone to configure a root zone server. You must also use a period as the zone name to create a root zone. Windows 2000 recognizes the period as a root zone and then configures the zone files correctly. Figure 4-8 shows the three zone type choices, while Figure 4-9 shows how to name a zone.

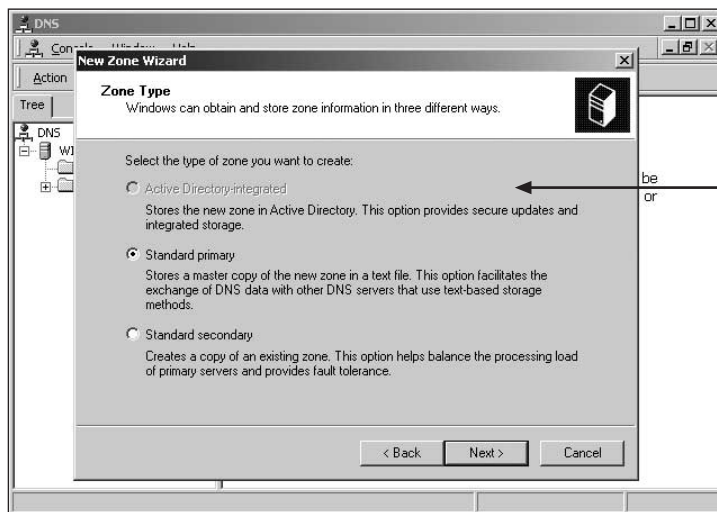


Figure 4-8 Types of zones

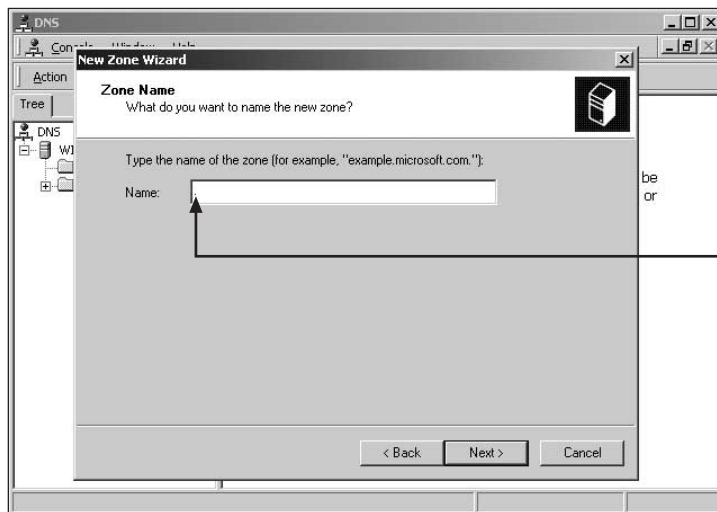


Figure 4-9 Naming a root zone

Figure 4-10 shows the zone files created by Windows 2000 when you name a zone file with a period.

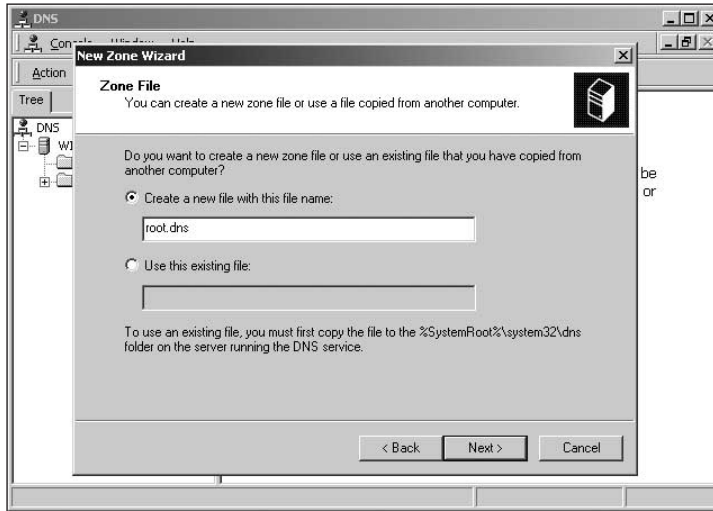


Figure 4-10 Root zone files created by Windows 2000

In Figure 4-10, the zone file name is `root.dns`, which signifies that Windows 2000 is creating a root zone for internal use.



If you create a root zone when your organization is not connected to the Internet and then you later connect to the Internet, you must remove the root zone or DNS queries may not occur correctly.

Configuring Primary and Secondary Zones

On DNS servers using standard DNS zones, you must configure primary and secondary servers with the appropriate zone files. If you wish to create a primary name server, you must configure the DNS server to use a standard primary zone. Figure 4-8 shows the different types of zone files: Active Directory integrated, standard primary, and standard secondary. If you select a standard primary zone, the first item you must configure is a name for the zone. You must place the entire domain name in as the primary zone file name. For example, to create a primary zone file for Course Technology, you need to place the name `course.com` in the primary zone file name.

Figure 4-11 shows a standard primary zone with the name `chap4.win2kbook.org`.

Windows 2000 appends `.dns` to the name you provide to create the DNS zone files for the zone. Figure 4-12 shows this default naming for `chap.4win2kbook.org`.

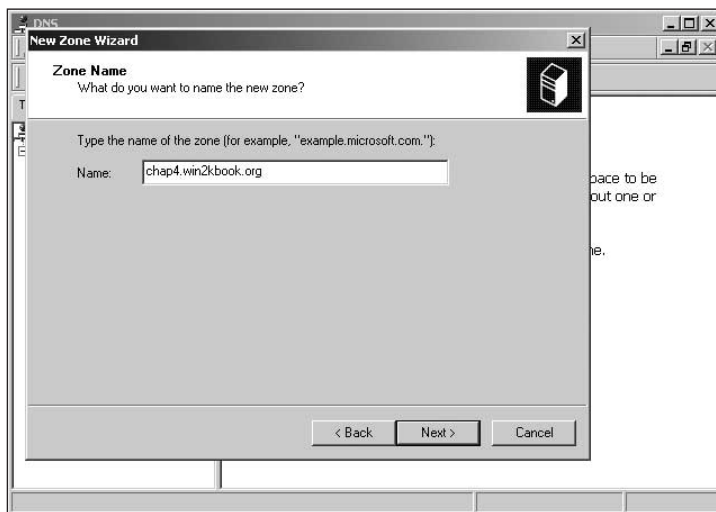


Figure 4-11 Naming a standard zone file

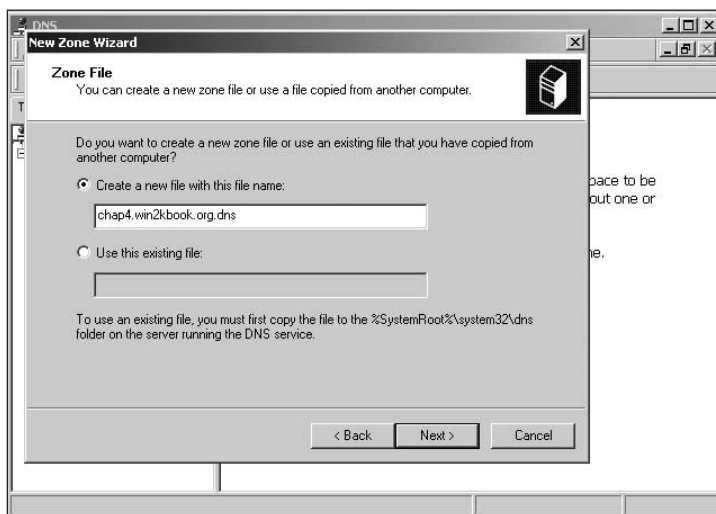


Figure 4-12 Default zone file naming

At this point, you configure a standard primary zone with the defaults and it's stored in the `\winnt\system32\dns` folder. A single DNS server can host as many standard primary zones as you want to configure. However, server resources limit the number of DNS zones.

Once you configure a primary zone, you may need to create a standard secondary zone on another DNS server in order to provide backup and faster responses to client DNS requests. Creating a standard secondary zone is very similar to configuring a standard primary zone. Right-click Forward Lookup Zones and select New Zone. Once you choose a standard

secondary zone and provide a zone name, you must choose a Master DNS server or servers to provide zone information to the secondary name server. In effect, the Master DNS server setting refers the standard secondary zone to the correct primary name server for the zone. Figure 4-13 displays the portion of the New Zone Wizard where you specify the Master DNS server.

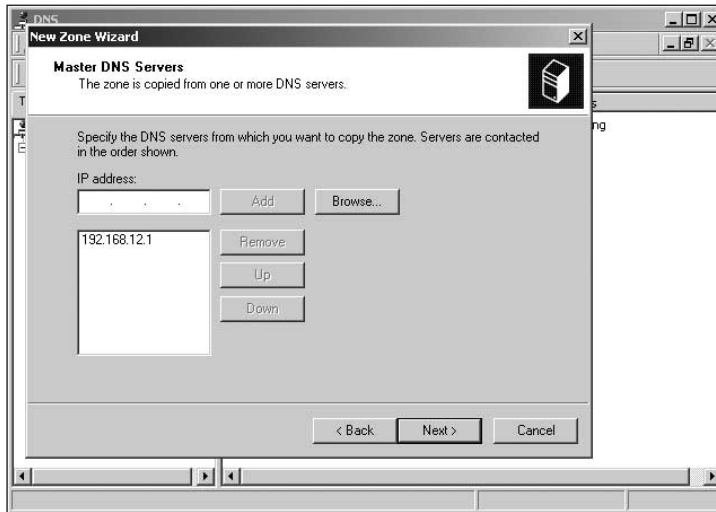


Figure 4-13 Configuring Master DNS servers

You can configure DNS servers to hold the primary zone file for one portion of the domain namespace and a secondary zone for another. Figure 4-14 shows a DNS server with a standard primary zone and a secondary zone configured. You should configure at least one primary and one secondary DNS zone for every standard DNS zone you create.

Active Directory integrated zones are stored in the Active Directory database and are automatically replicated when AD information is replicated. As a result, administrators do not have to configure zone replication for fault tolerance. Instead, the same services that replicate AD information handle replication of all DNS information within a zone. The problem with AD integrated zones comes from the problems of coexistence with UNIX-based DNS servers or other non-Windows 2000 servers.

If your network consists of Active Directory integrated zones only, you do not need to configure primary and secondary zones. Instead, all Active Directory DNS zones are replicated via the same mechanisms as the Active Directory itself.

Configuring Caching-only Servers

Many remote offices need to resolve host names via DNS. In very small offices, it may be possible to allow client DNS requests to pass over the WAN link to a DNS server located at the central office. Figure 4-15 shows a remote office where all DNS requests must pass over the WAN link.

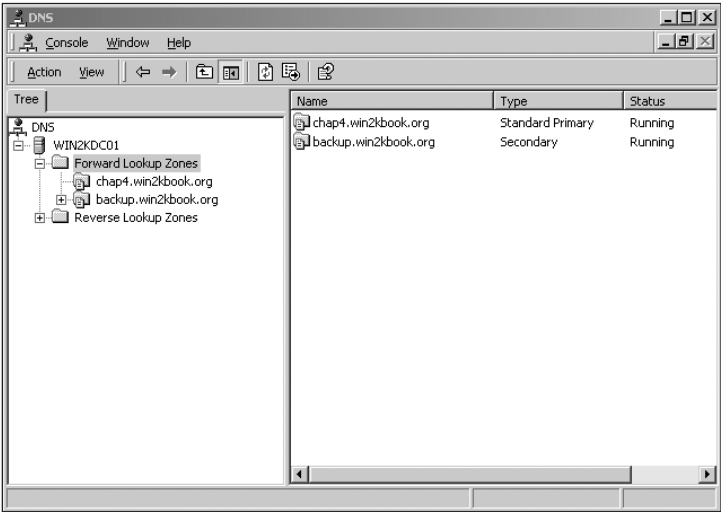


Figure 4-14 DNS server with a primary and secondary zone

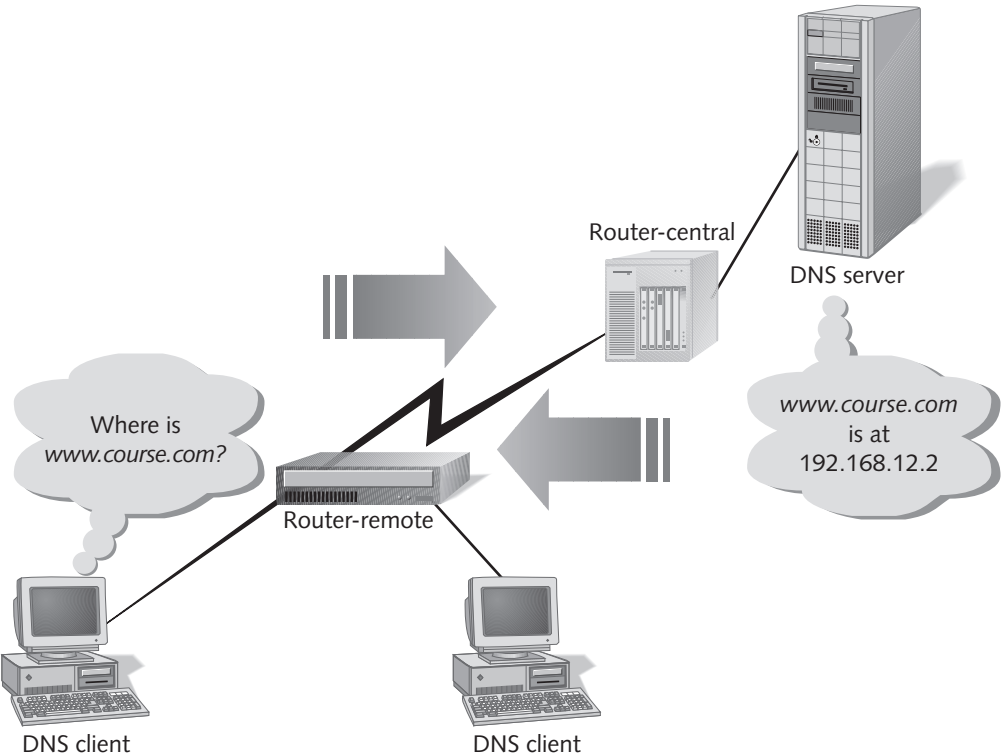


Figure 4-15 Remote office and DNS

With only a few clients at the remote office, the DNS traffic is normally not enough to affect the available bandwidth between the remote office and the central office. As the number of clients at the remote office increases, the traffic may overwhelm a slow WAN link. If the number of clients is high or the company expects rapid growth, you should place a caching-only server at the remote location. The caching-only server is not authoritative for any particular DNS zone, that is, it is not configured to hold a primary or secondary zone. However, as its name implies, it forwards DNS requests and then caches the DNS resolutions.

The process of creating a caching-only server consists of loading the DNS server service and then configuring forwarder addresses. Right-clicking the server in the DNS console, selecting Properties, and clicking the Forwarders tab allows you to configure the forwarder addresses. Figure 4-16 displays the Forwarders tab.

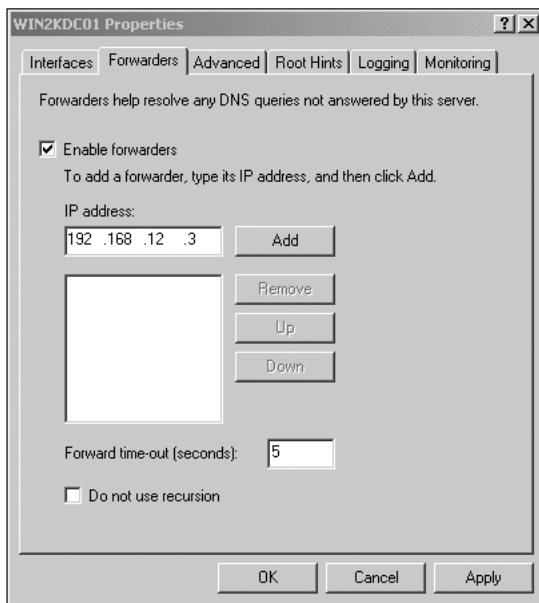


Figure 4-16 Configuring DNS forwarders

Implementing a Delegated Zone for DNS

Many networks use subdomains to break the DNS namespace into more manageable units. After creating subdomains, it is possible to delegate authority for a zone via the New Delegation Wizard. To access the New Delegation Wizard, right-click the zone or subdomain you wish to delegate, and select New Delegation. You are prompted for the name of the domain you want to delegate and the IP address or name of the DNS server to hold the delegation. Then select the person or group to whom you wish to delegate and assign the appropriate permissions.

Configuring Zones for Dynamic Updates

As mentioned earlier in this book and this chapter, Windows 2000 DNS supports dynamic registration of client A and PTR records. However, by default, standard zones on Windows 2000 DNS servers do not support dynamic registration. To configure a standard zone to accept dynamic updates, right-click the zone, select Properties, and then select Yes in response to “Allow dynamic updates?” Figure 4-17 displays the correct setting for dynamic updates.

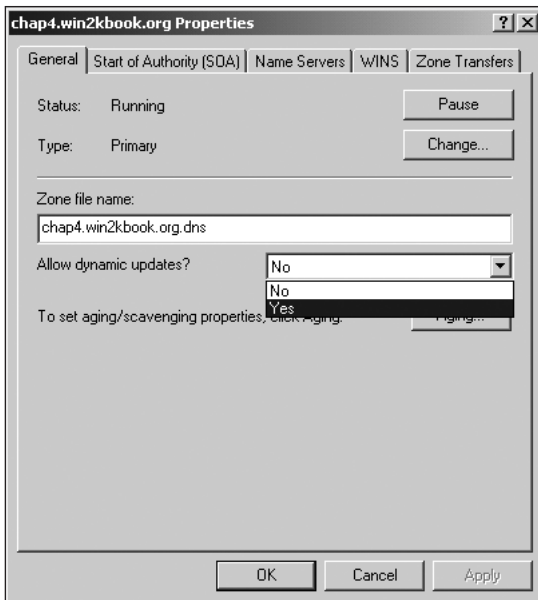


Figure 4-17 Configuring dynamic updates

Once the zone can accept dynamic updates, Windows 2000 clients automatically register A records and, if they are configured as DHCP clients, request that the DHCP server register PTR records. Non-Windows 2000 clients cannot automatically register either A records or PTR records with a DNS server configured for dynamic updates. To allow dynamic updates for these clients, you can configure the DHCP server to register DNS A and PTR records automatically for non-Windows 2000 clients. Figure 4-18 shows the DHCP console and the DNS dialog box for setting DHCP interaction with DNS.

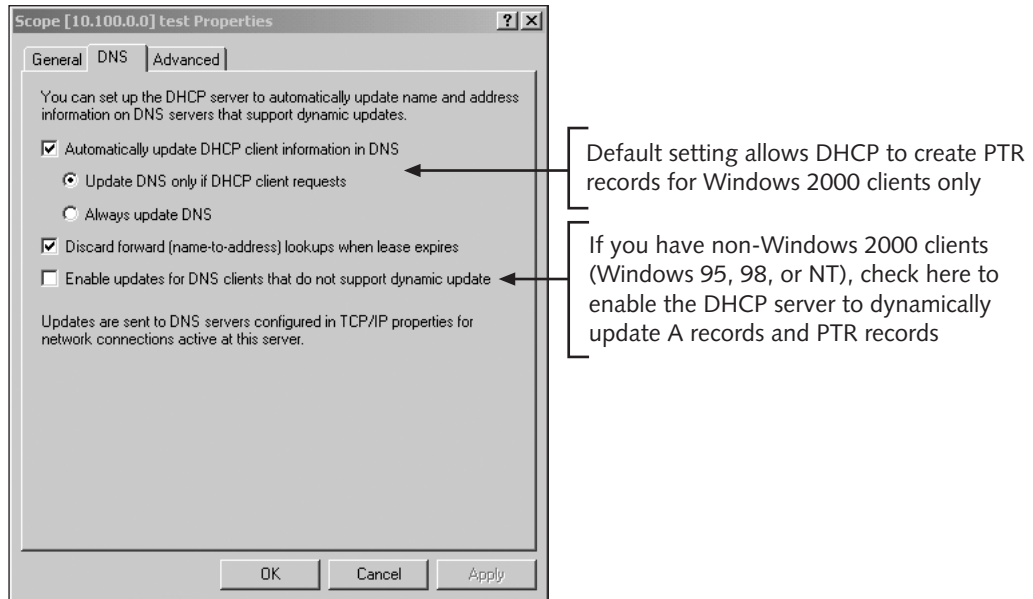


Figure 4-18 DHCP configuration for automatic DNS updates

CREATING RESOURCE RECORDS MANUALLY

Although Windows 2000 clients can automatically register A records, and A records and PTR records can automatically be registered through DHCP, it is still necessary to create many resource records manually.

To create a record manually you right-click the zone in which you wish to create a record and select one of the listed records or the Other New Records option. Figure 4-19 shows the options available.

Using the dialog box that opens, you can create resource records ranging from host or A records to service records. The number and type of manual records that you must create vary for each network, but at a minimum you must configure canonical names, or CNAMEs, for Web servers.

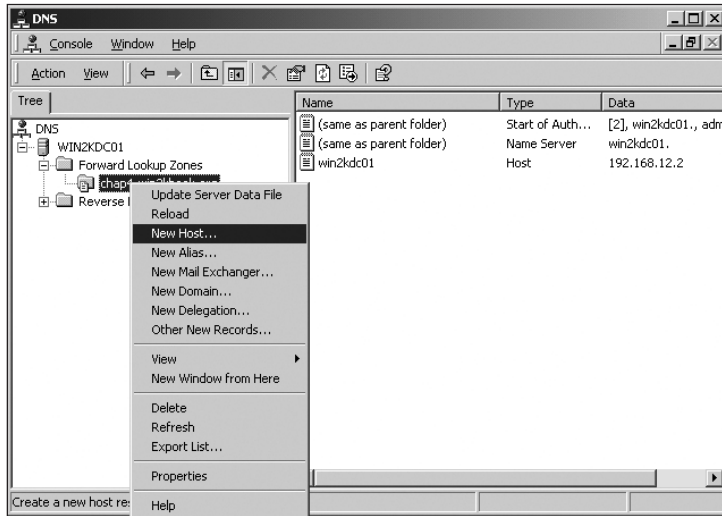


Figure 4-19 Manual resource record creation

DNS CLIENT CONFIGURATION

Once you correctly install and configure your DNS servers, you need to configure the clients on the network so they can use the DNS servers. How you configure the client depends on whether the client is configured with a static IP address or is a DHCP client.

For clients with static IP addresses, you must manually configure a Preferred DNS server and an Alternate DNS server in the TCP/IP properties DNS configuration tab for Windows 95 and 98 clients. Figure 4-20 shows the basic manual DNS configuration for Windows 2000 clients.

If you need to configure more than two DNS servers on a client, click the Advanced button at the bottom of the Internet Protocol (TCP/IP) Properties dialog box shown in Figure 4-20. Figure 4-21 displays the DNS tab in the Advanced TCP/IP Settings dialog box. Here you can add additional DNS servers and prioritize the order of use of DNS servers.

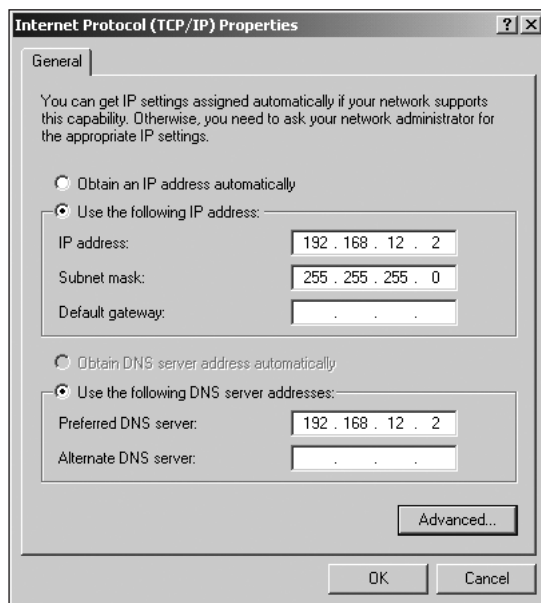


Figure 4-20 Configuring DNS settings manually

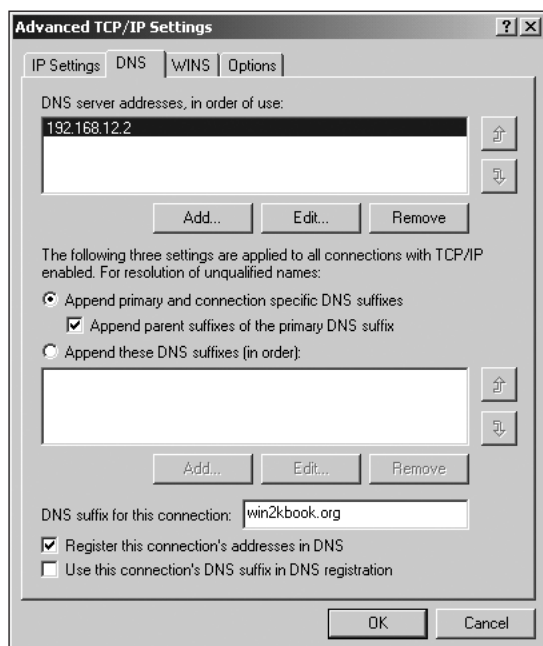


Figure 4-21 Advanced manual DNS configuration

If your clients use DHCP, configuring DNS for them is much easier. You need to configure the DNS options for the scope that the client will obtain an IP address from. Chapter 3 discusses how to perform this task.

MANAGING, MONITORING, AND TROUBLESHOOTING DNS

4

Overall, if installed and configured correctly, DNS servers and clients normally require very little administration. Still, problems can and do arise with all networking components. Therefore, you must know how to manage, monitor, and troubleshoot DNS.

Setting TTL Properties

All DNS servers maintain a cache of information that contains the resolutions they performed for clients. This cache speeds the DNS resolution process because the DNS server can pull information from this cache instead of performing an entire DNS query. Cache entries are maintained for a length of time determined by the time-to-live setting of the zones on a server. Figure 4-22 shows the Time To Live, or TTL, for a forward lookup zone. By default, the TTL is one day. You can open the dialog box shown in Figure 4-22 by right-clicking a zone in the DNS console and selecting Properties, and then selecting the Start of Authority (SOA) tab.

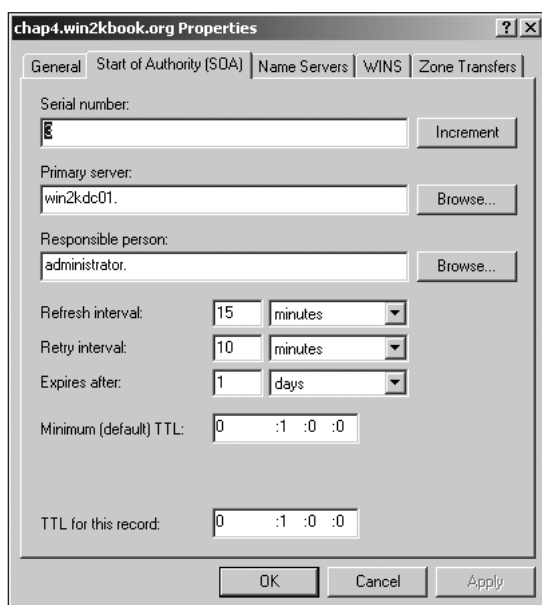


Figure 4-22 Setting TTL for a zone

The minimum (default) TTL setting specifies the amount of time a server can cache information in a zone. Other items of importance in Figure 4-22 are the Refresh interval, which determines how often secondary servers contact their primary server to update zone information; and the Retry interval, a wait period the secondary server uses if it cannot contact a zone's primary server. You may want to increase the TTL if your computer name to IP address mapping does not change often. In addition, the serial number in Figure 4-22 is the number used to determine if changes have occurred on the primary zone. The primary name server and secondary name servers compare this serial number to ensure that they are using the same zone files. If the primary name server has a newer version of the database (one with a higher serial number), the secondary servers know that they need to update their zone files.

Zone Transfer Settings

If you use standard primary and secondary name servers, you may also want to configure additional zone transfer settings to ensure optimal exchange of database information.

Figure 4-23 shows the Zone Transfers tab originally shown as the last tab in Figure 4-22. In this dialog box, you can configure how zone transfers occur (You must allow zone transfers to occur between primary and secondary servers.) Within this same tab, you can also configure exactly what servers can be involved in the zone transfer process. Specifying that only certain servers can participate in zone transfers increases the security of all DNS transactions.

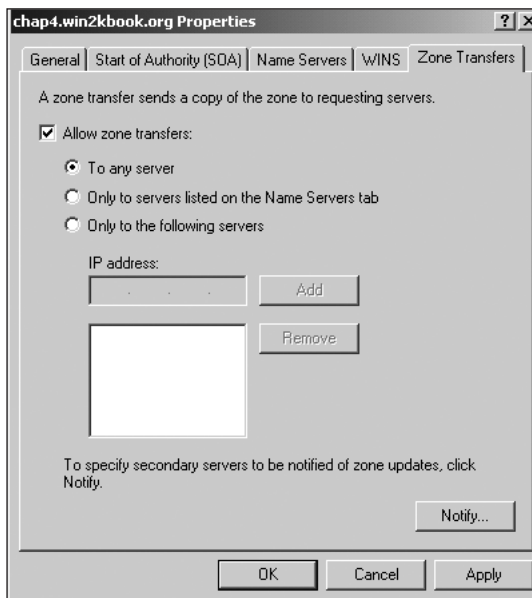


Figure 4-23 Zone transfer settings

Configuring the exact IP addresses or names of the servers that can participate in zone transfers ensures that all DNS information sharing is secure because only servers you specify can participate in zones transfers.

Monitoring and Testing Tools

Another administrative task is testing and logging DNS server activity. Windows 2000 provides two test utilities for this purpose: a simple graphical tool and the nslookup utility.

To access the simple graphical tool, right-click the server name in the DNS console and select Properties. Figure 4-24 displays the monitoring tool you can access via the Monitoring tab.

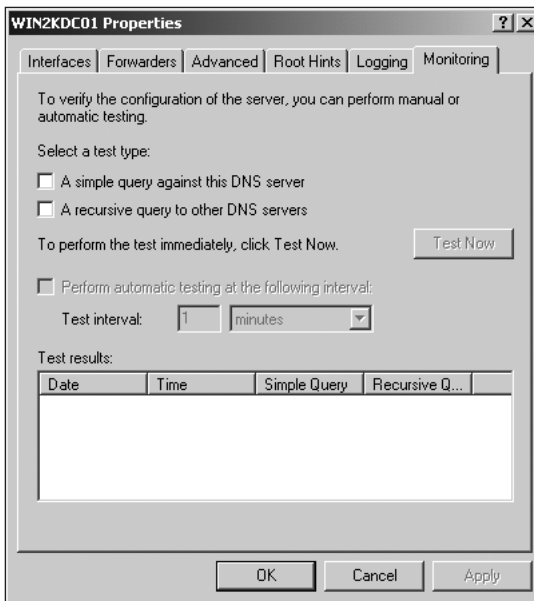


Figure 4-24 Monitoring a DNS server

Using the monitoring tool, you can perform a simple query that attempts a forward lookup query. The tool also allows you to perform a recursive query. Finally, you can perform the test immediately with the Test Now button, or you can have the tests occur automatically at a preset interval. With this tool, you can quickly determine the status of the DNS server. For more detailed logging and information, you can use the DNS log in EventViewer. Also, as an administrator, you can configure the logging options on the Logging tab shown in Figure 4-24. Figure 4-25 shows the Logging options and the default path for the log file. Use with discretion: As with all logging, the more items you log, the more overhead you place on the DNS server.

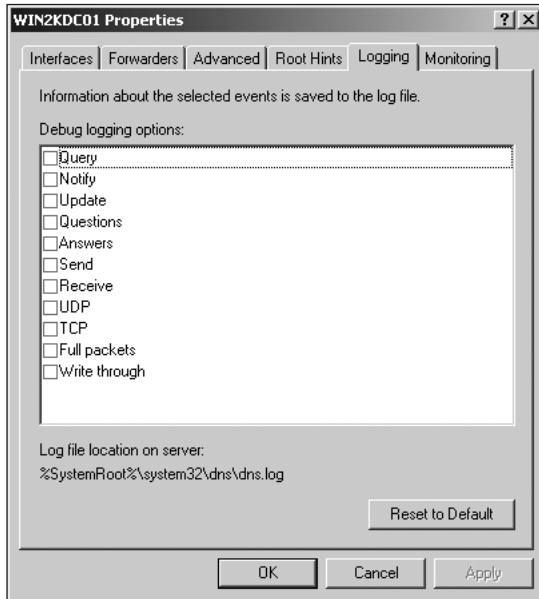


Figure 4-25 DNS logging

Additionally, you can use the `nslookup` utility to verify that a DNS server is available and that resource records have been created for the zone. You can use `nslookup` to perform a single lookup in non-interactive mode, or you can perform a series of lookups in interactive mode. To perform a single lookup, you must type the following after the command prompt:

```
nslookup [DNS name] [DNS server]
```

In the non-interactive syntax, you should replace the DNS variable with the DNS name you want to query the DNS server for. The DNS server is the server on which you wish to check the resource record. Also, instead of the DNS server name, you can use the IP address of the DNS server you want to query. The following shows a successful `nslookup` of the resource record for server `win2dc01`:

```
F:\>nslookup win2kdc01 192.168.12.2
Server:  win2kdc01.chap4.win2kbook.org
Address:  192.168.12.2

Name:     win2kdc01.chap4.win2kbook.org
Address:  192.168.12.2
```

From this `nslookup`, you can see that the DNS name and the DNS server being checked for resource records are the same machine.

You can also use `Nslookup` in interactive mode. Use this mode if you plan to enter multiple lookups. To enter interactive mode, type `nslookup` after the command prompt and press **Enter**. You can then use the `?` to access help and information about the many different

nslookup options available. The following shows how to enter interactive mode and the results of the help command:

```
F:\>nslookup
Default Server: win2kdc01.chap4.win2kbook.org
Address: 192.168.12.2

> ?
Commands: (identifiers are shown in uppercase, [] means
optional)
NAME - print info about the host/domain NAME
using default server
NAME1 NAME2 - as above, but use NAME2 as server
help or ? - print info on common commands
set OPTION - set an option
all - print options, current server and host
[no]debug - print debugging information
[no]d2 - print exhaustive debugging
information
[no]defname - append domain name to each query
[no]recurse - ask for recursive answer to query
[no]search - use domain search list
[no]vc - always use a virtual circuit
domain=NAME - set default domain name to NAME
srchlist=N1[/N2/.../N6] - set domain to N1 and search
list to N1,N2, etc.
root=NAME - set root server to NAME
retry=X - set number of retries to X
timeout=X - set initial time-out interval to X
seconds
type=X - set query type (ex. A,ANY,CNAME,MX,
NS,PTR,SOA,SRV)
querytype=X - same as type
class=X - set query class (ex. IN
(Internet), ANY)
[no]msxfr - use MS fast zone transfer
ixfrver=X - current version to use in IXFR
transfer request
server NAME - set default server to NAME, using current
default server
lserver NAME - set default server to NAME, using initial
server
finger [USER] - finger the optional NAME at the current
default host
root - set current default server to the root
ls [opt] DOMAIN [> FILE] - list addresses in DOMAIN
(optional: output to FILE)
-a - list canonical names and aliases
-d - list all records
```

```

        -t TYPE      - list records of the given type (e.g. A,
                        CNAME,MX,NS,PTR etc.)
view FILE          - sort an 'ls' output file and view it
                    with pg
exit              - exit the program

```

```
>
```

The > prompt signifies interactive mode. A very useful command in interactive mode is the `ls` command. Using this command, you can list all the A records with the `-a` switch, all records with the `-d` switch, and a particular type of record with the `-t` (type) switch. The following output show the results of each of these command-switch combinations being run in interactive mode:

```

F:\>nslookup
Default Server:  win2kdc01.chap4.win2kbook.org
Address:  192.168.12.2

> ls -a chap4.win2kbook.org
[win2kdc01.chap4.win2kbook.org]

> ls -d chap4.win2kbook.org
[win2kdc01.chap4.win2kbook.org]
chap4.win2kbook.org.          SOA win2kdc01.chap4.win2kb
                                ook.org administrator
                                or. (9 900 600 86400 3600)

chap4.win2kbook.org.         NS  win2kdc01.chap4.win2kb
                                ook.org

win2kdc01                    A   192.168.12.2
win2kdc02                    A   192.168.12.3
win2kdc02                    MX  10   win2kdc02.chap4.w
                                in2kbook.org

chap4.win2kbook.org.         SOA win2kdc01.chap4.win2kb
                                ook.org administrator
                                or. (9 900 600 86400 3600)

> ls -t mx chap4.win2kbook.org
[win2kdc01.chap4.win2kbook.org]
win2kdc02                    MX  10   win2kdc02.chap4.win2k
                                book.org

>

```

Using this command and its switches, you can verify that the resource records do indeed exist in the DNS zone file.

CHAPTER SUMMARY

- ❑ Windows 2000 provides a full-featured DNS server that allows an administrator to create, maintain, and deploy a standards-based DNS infrastructure. Windows 2000 also supports the use of older methods of DNS name resolution, such as host files.
- ❑ DNS is a hierarchical system used to create a system that can resolve host name to IP address mapping. In Windows 2000, DNS is the primary name resolution method. The service is required on all Windows 2000 networks using Active Directory.
- ❑ You can easily start and configure the Windows 2000 server service to support standard and secondary zones with corresponding zone files stored on the server's hard drive. With primary and secondary zones, the DNS server is configured as a primary name server for a particular zone or as a secondary or back-up, name server for a zone. It is also possible for a DNS server to be the primary server for one zone and the secondary server for another.
- ❑ Additionally, Windows 2000 supports new Active Directory integrated zones that allow storage and replication of the DNS database within the AD database. Active Directory integrated zones ease the administrative tasks associated with manually setting up replication between primary and secondary name servers.
- ❑ All zones within Windows 2000, once configured to accept them, allow for dynamic DNS updates. Once configured to accept dynamic updates, all zones can allow Windows 2000 computers to create their own A records. Also, if your network uses DHCP, you can configure the DHCP servers to register PTR records for Windows 2000 clients and A and PTR records for non-Windows 2000 clients.
- ❑ You can manage, monitor, and troubleshoot DNS with the DNS console tool or the nslookup command-line tool. The DNS console allows an administrator to set most of the properties associated with the DNS server, including TTL, forwarders, and other configurations. The nslookup command allows an administrator to query DNS servers for information about resource records within the DNS database.

KEY TERMS

active directory integrated zones — DNS zones stored in the Active Directory database and replicated along with other Active Directory information.

authority — Ability to control what resource records, subdomains, and other attributes are associated with a particular DNS domain.

caching-only servers — DNS server configured without any zone files; a caching-only server contains IP addresses of DNS servers it can query to answer client requests and then store the information in a local cache.

DNS zone file — Text file, stored on a DNS server, that contains all information and resource records for a particular zone.

DNS zones — Portion of the DNS namespace that can be administered as a single unit.

Domain Name System (DNS) — Hierarchical naming system used to resolve host name to IP address mapping. It contains resource records.

forward lookup zones — DNS zone files that hold resource records that map host names to IP addresses. (They can also hold various other resource records.)

hostname — Command used after the command prompt to display the host name of the local machine.

host names — Common names given to network devices to allow users to interact with a name instead of an IP address.

host files — Text files that contain host name to IP address mapping; used to perform host name to IP address resolution. Precursor to the DNS system.

in-addr.arpa — Name given to the reverse lookup zone file.

Internet Service Providers (ISPs) — Companies that provide access to the Internet backbone.

inverse query — DNS query attempting to resolve a host name from a known IP address.

iterative query — DNS query to which the server responds with the best answer it can provide or by forwarding the request to another name server and then returning an answer.

LMHOSTS — Text file mapping NetBIOS names to IP addresses; precursor to WINS service.

name registration company — Company with the authority to register DNS domains within the DNS namespace.

primary name servers — DNS servers that hold a read/write copy of the zone file for a particular DNS zone; control replication with secondary name servers.

recursive query — DNS query which asks the server to respond either with the DNS information or an error message stating that it does not have the information; used between clients and DNS servers.

reverse lookup zone — Special DNS zone that holds PTR records, IP address to host name mapping.

root name servers — Servers that hold information about the overall Internet domain name servers.

secondary name servers — DNS servers that hold read-only copies of a zone file for a particular DNS zone; accept updates to the DNS zone file only from configured primary name servers.

Windows Internet Name Service (WINS) — Windows 2000 service that provides a dynamic database of NetBIOS name to IP address mapping.

zone of authority — Portion of the DNS namespace that an organization controls.

zones transfers — Copying zone file information from primary name servers to secondary name servers.

REVIEW QUESTIONS

1. Which one of the following holds a read/write version of DNS zone files?
 - a. Domain Master Name server
 - b. Primary name server
 - c. Caching-only name server
 - d. Secondary name server
2. A(n) _____ record maps a host name to an IP address.
3. Which one of the following occurs at the beginning of a DNS zone file and provides important information about what servers are authoritative and contact information?
 - a. CNAME record
 - b. NS record
 - c. SOA record
 - d. SRV record
4. Which one of the following lists the six steps in host name resolution in correct order?
 - a. LMHOSTS file, local host name, HOSTS file, DNS server, WINS server, broadcast
 - b. HOSTS file, local host name, DNS server, WINS server, broadcast, LMHOSTS file
 - c. Local host name, HOSTS file, DNS server, WINS server, broadcast, LMHOSTS file
 - d. DNS server, local host name, HOSTS file, WINS server, broadcast, LMHOSTS
5. If your company has the ability to create subdomains within your assigned domain from a name registration company, your company is considered _____ for that domain.
6. A query that must be answered with the best response a server has in its DNS files or with an error message stating that the query cannot be completed is considered:
 - a. Recursive
 - b. Iterative
 - c. Authoritative
 - d. Best-guess
7. To find a host name from a known IP address, you must perform a(n) _____ query.
8. Which one of the following resource records allows you to assign an alias or common name to a machine?
 - a. A record
 - b. MX record
 - c. SRV record
 - d. CNAME record

9. What types of DNS zones does Windows 2000 support? (Choose all that apply.)
 - a. Standard primary zones
 - b. Standard secondary zones
 - c. Active Directory integrated zones
 - d. All of the above
10. You must manually configure zone replication when using Active Directory integrated zones. True or false?
11. The portion of the namespace that a server is responsible for is called its _____.
12. Forward lookup zones contain:
 - a. IP address to host name mapping
 - b. No host name to IP address mapping
 - c. MX records only
 - d. Host name to IP address mapping
13. The new DNS record used by Windows 2000 to locate domain controllers is the _____ record.
14. Which of the following can automatically register A records and PTR records once a DNS zone has been configured for dynamic updates?
 - a. Windows 2000 clients
 - b. Windows 95 clients
 - c. Windows 98 clients
 - d. None of the above
15. Which of the following tools can you use to monitor DNS? (Choose all that apply.)
 - a. DNS console
 - b. Active Directory users and computers console
 - c. Nslookup
 - d. Hostname command
16. In order for non-Windows 2000 clients to use DDNS, the DHCP server service must be configured to register A and PTR records dynamically. True or false?
17. Which one of the following DNS servers is not authoritative for any particular zone and is used to reduce DNS resolution traffic to remote sites?
 - a. Active Directory integrated server
 - b. Caching-only server
 - c. Secondary name server
 - d. Primary name server

18. By default, all standard zones on Windows 2000 DNS servers automatically accept dynamic updates. True or false?
19. Nslookup can be run in either _____ mode or _____ mode.
20. The _____ is the amount of time that a DNS server caches information about a successful DNS query.

HANDS-ON PROJECTS

All Hands-on Projects in this chapter require two computers set up as described in the lab set-up section in the front of this book. For these exercises, you use the PCs named win2kdc01 and win2kdc02. To complete these exercises, you must have completed Hands-on Project 3-1 in Chapter 3. After completing the exercises in Chapter 3, win2kdc02 is already running DNS.



Project 4-1

To make win2kdc01 a member server in the win2kclass02.org domain:

1. Right-click **My Network Places** and click **Properties** to open the Network and Dial-up Connections dialog box.
2. Click **Advanced** and then click **Network Identification**.
3. Click the **Properties** button.
4. Select the **Domain** radio button, and then type **win2kclass02.org**. Click **OK**. If prompted for a username and password, enter the administrator name and password.



Under the TCP/IP properties for win2kdc01, you must configure the primary DNS as the IP address of win2kdc02 or the machine cannot join the domain.

5. Click **OK** to close the Welcome to win2kclass02.org domain dialog box.
6. Click **OK** to close the dialog box that states that you must restart your machine.
7. Click **OK** to close the Systems Properties dialog box.
8. Click **Yes** to restart your computer.



Project 4-2

To install the DNS server service on the server win2kdc01 and configure it as a caching-only server:

1. Log on to the **win2kclass02** domain as **Administrator** with the password **password**.
2. Right-click **My Network Places** and click **Properties** to open the Network and Dial-up Connections dialog box.

3. Click **Advanced** and then select **Optional Networking Components**.
4. Double-click **Networking Services** to display a list of available services.
5. Click in the box to the left of the **Domain Name System (DNS)** item, and then click **OK**.
6. Click **Next** to install the DNS server service. If prompted, provide a static **IP** address for the server.

You may be prompted to insert your Windows 2000 server CD-ROM.

You installed the DNS server service on win2kdc01. At this point, if you do not add any zone files to the server, and you verify that the root hints (available on the Root Hints tab when you right-click the server and select Properties) are configured, the server acts as a caching-only server.



Project 4-3

You must perform this exercise on win2kdc01.

To configure a root name server:

1. Click **Start, Programs, Administrative Tools, DNS** to start the DNS console.
2. Once the DNS console starts, expand the tree under win2kdc01 by clicking the **+** next to the server name.
3. Click to select **Forward Lookup Zones**.
4. Right-click **Forward Lookup Zones** and then select **New Zone**.

This begins the New Zone Wizard.

5. Click **Next**.
6. Ensure that the **Standard Primary** radio button is selected, and then click **Next**.
7. Type a period in for the name of the zone. Click **Next**.
8. Accept the default zone file name of **root.dns**, and then click **Next**.
9. Click **Finish**.

If you see a new zone represented by a folder with the name **.**, you successfully configured a root name server.

10. **Right-click** on the root zone (zone named **.**), and then click **Delete**. Click **OK** to confirm deletion.



This step is necessary to ensure that the following Hands-on Projects work correctly. You would not perform this step in a real-world configuration of a root name server.



Project 4-4

To configure a primary zone on the server win2kdc02:

1. Click **Start, Programs, Administrative Tools, DNS** to start the DNS console.
2. Once the DNS console starts, expand the tree under win2kdc02 by clicking the + next to the server name.
3. Click to select **Forward Lookup Zones**.
4. Right-click **Forward Lookup Zones**, and then select **New Zone**.
This begins the New Zone Wizard.
5. Click **Next**.
6. Ensure that the **Standard Primary** radio button is selected, and then click **Next**.
7. For the zone name, use **project44**. Click **Next**.
8. Accept the default zone file name of **project44.dns**, and then click **Next**.
9. Click **Finish** and you see a new zone represented by a folder with the name **project44**.



Project 4-5

To add resource records manually to a DNS zone:

1. On the server win2kdc02, open the DNS console, expand the DNS zone information, and then click to select the **project44** zone file.
2. Right-click **project44** and then select **New Host**.
3. In the New Host dialog box, type **win2kdc01** for the host name and use **192.168.12.1** as the IP address.
4. Click **Add Host** to add the **A record** to the project44 zone file.
5. Repeat Steps 3 and 4 for **win2kdc02** using the IP address of **192.168.12.2**.

You can add all other resource records using the same series of steps listed in this Hands-on Project.



Project 4-6

To configure a zone for dynamic updates:

1. On the server win2kdc02, open the DNS console, expand the DNS zone information, and then click to select the **project44** zone file.
2. Right-click **project44** and then select **Properties**.
3. In the **Allow Dynamic Updates** box, select **Yes**.



On an Active Directory integrated zone, you have three possible choices in the Allow Dynamic Updates box: only secure updates, yes, and no.

4. Click **OK**.

You configured the zone to accept dynamic updates.



Project 4-7

To test the DNS server service using the tools in the DNS console:

1. Open the DNS console on win2kdc01.
2. Right-click the server **win2kdc01** and select **Properties**.
3. Click the **Monitoring** tab and ensure that the check boxes for a simple query and a recursive query are selected.
4. Click **Test Now** to test the server.

You should see the results at the bottom of the dialog box in the area labeled “Test results”.



You can also set up automatic testing at a certain time interval by clicking Perform automatic testing at the following interval: and selecting an interval.

CASE PROJECTS



Case 1

Your company consists of a central office of nearly 500 computers and 50 servers. You also have four remote sites connected to the central office via ISDN connections. Your boss asks you to design a DNS architecture for the company that meets the needs of the central office and the remote sites. Create a one-page document detailing your plans for the company's DNS servers.



Case 2

A company called Hogan Industries currently uses UNIX servers to host its DNS servers. The company is in the process of migrating to a full Windows 2000 network, but there are some concerns about replacing the UNIX DNS servers. You are asked to create two proposals: one for replacing the UNIX DNS servers completely with Windows 2000 DNS servers and another proposal for keeping the current UNIX DNS servers and integrating Windows 2000 DNS servers. Using the Microsoft Web site at www.microsoft.com and other resources, research the pros and cons of each proposal and then create a summary of each in a two- to three-page paper.



Case 3

As the senior engineer for Freytech Inc., one of your major tasks is providing training for new hires and existing junior engineers. For this month's training meeting, you are asked to discuss DDNS and its implementation in Windows 2000. Prepare a 15- to 30-minute training session on the Windows 2000 implementation of DDNS.